Information Security Advisory Committee
Report on Committee Activities in 2012-2013 Academic Year

September 20, 2013

The Information Security Advisory Committee (ISAC) was constituted by the Academic Senate in 2012 to advise the University of Texas at Dallas Information Security Officer in planning and testing measures to provide security of the universitys information resources in such a way as to comply with UT System security requirements for university information.

Appointment of the following members of the faculty was approved by the Senate in their meeting on November 28, 2012: Ravi Prakash (Chair), Dinesh Bhatia, Kevin Hamlen, Joe Izen, Tim Redman and Tres Thompson.

The loss and theft of a few laptops of some researchers has triggered extreme measures by the UT System to ensure confidentiality of data. All campuses have been mandated to implement full hard-disk encryption for all laptop computers. On each campus it is the responsibility of the President and the Chief Information Security Officer (CISO) to ensure that the mandate is implemented in a timely manner.

Over two meetings and multiple rounds of email exchanges the ISAC compiled a list of questions that were posed to the campus CISO on February 22, 2013. Responses to these questions were requested within two weeks. The CISO's responses were received on March 4, 2013. Based on its deliberations and the responses received from the CISO, ISAC reached the following conclusions:

1. Faculty input was not sought in formulating the security mandate. Domain experts doing research in the area of information security were not consulted.

2. Faculty members use laptop computers for a variety of tasks, including teaching and research. Sometimes the laptop computer is the instrument used to gather live research data. There are instances where the laptop computer itself is the research subject. However, while formulating the mandate only a generic use-case scenario appears to have been considered, namely that of the laptop being used for general purpose document preparation, email communication and web access only.

3. A scientific performance evaluation of the encryption software was never conducted. A number of older laptop computers had to be decomissioned. Relatively new machines have taken a performance hit. Some useful capabilities have been disabled. The ability of vendors to service laptop computers has been severely compromised. Claims were made by the CISO that there was no performance degradation. However, the committee found no support for this claim by any reputed, independent, product-testing organization, and believes that this claim is based on marketing hype promulgated by one hardware manufacturer. Any assessment of the cost of this mandate, both in terms of hardware obsolescence and productivity loss, is at best unreliable and inadequate.

4. Full disk encryption implementation plan, as proposed by the CISO, was centralized and non-scalable. All requests for exemption from disk encryption had to be ultimately approved by the UT System. As per the CISO, decisions on exemption requests were to be notified within a month. In early April

of 2013, even the fact that exemption requests can be made was not known to most members of the faculty. Yet, with a very limited number of exemption requests to process, the UT System had been unable to meet its decision making timeline. Exemption requests from two members of the committee took significantly longer to process: six months in one instance, and two months in the other.

A *one-size-fits-all* solution for data security across all UT System campuses is ill-advised. On any campus, it deprives the faculty, President, and the CISO of the opportunity to work together to devise a solution that is most suited for the needs of that campus. Such a solution will have (and is already having) an immediate, deleterious, and potentially catastrophic impact on certain university activities that do not match the limited use-case scenario considered by the mandate – most notably scenarios that involve research.

In its April 10, 2013 meeting ISAC shared the concerns mentioned above with the CISO and CIO of the university as well as with Mr. Lewis Watkins, CISO of UT System. ISAC members argued that members of the faculty routinely work with toxic chemicals, pathogens, radioactive material, etc. and a number of university-wide committees maintain oversight on such activities. To date these committees been very effective in developing sensible solutions that meet the unique needs of UT Dallas. Hence, ISAC should be modeled along the lines of the following committees:

- Institutional Biosafety and Chemical Safety Committee,
- Institutional Animal Care and Use Committee, and
- Radiation Safety Committee

The UT System CISO and UTD CIO agreed with the need to address the issue of information security in general, and laptop encryption in particular, with the involvement of the faculty, leveraging their expertise, and sensitive to their research and teaching needs.

In its meeting on May 15, 2013 the Academic Senate amended ISAC's charge to reflect that approval/non approval of laptop encryption requests be made at the local level, and not at the system level. Membership of ISAC was also expanded to include two external domain experts.

In conclusion, ISAC has worked diligently to ensure that the teaching and research needs of UTD faculty are safeguarded when information security solutions are developed and implemented. The committee has had an excellent working relation with the university CIO. We look forward to working in a collaborative and collegial manner with the newly appointed Director of Information Security.